E-MAIL GUIDELINES

January 22, 2009

PURPOSE AND INTENT

- In light of the prevalent nature of e-mail systems in Utah State government, and as a result of good business practices, legislation and litigation, the ability to appropriately store, manage, and purge the e-mail of State of Utah employees has become imperative. E-mail is quickly becoming the main method of communication in many areas of state government. It is now an official record of what has transpired in many areas. At the same time, it is used for non-official purposes such as personal messages and transitory matters. All of this information typically is stored in e-mail systems and on backup tapes without regard to need, importance or content, kept for the same length of time, then purged, again without regard to need, importance or content. Several problems arise from these circumstances:
- Records of value—those needed by an agency to document its own actions or make decisions based on that information or which provide accountability to the public—are not placed where their survival can be guaranteed. Such records often have historical research value after a period of time or are needed for litigation.
- E-mails of no value are kept, often in multiple places, and then take up server space, cause unnecessary expense in keeping them and interfere with attempts to find valuable records.
- E-mail originates with a single user, though it may be sent to many recipients. In turn, it may be forwarded by original recipients to further recipients, thus creating a trail of duplicates that is difficult to manage and typically unnecessary from a records management perspective.
- E-mails that are deleted from an in or out box by a user often still exist on backup tapes or in other servers. If at any time one message needs to be retrieved, finding the item may be next to impossible without restoring several years' worth of old deleted (and worthless) e-mail.
- Backup systems are not record-keeping systems; however, they are often forced into that role, causing technical staff—with their high salaries—to be redirected from mission-critical projects to coax the backup system into doing something for which it was not designed. Backup systems ideally should only be used for disaster recovery.
- Records of value, even if kept by the creator, usually are not in a centralized location accessible to others in the agency that may need the information.

The technology required to effectively manage e-mail records is now widely available and is quickly expanding in terms of the scope and efficiency of services offered. As State correspondence becomes more and more electronically based, the availability of such products makes it possible, and necessary, to institute a sound and comprehensive e-mail management policy. Acknowledging that records management needs, workloads, and complexity vary widely across State government, the intent is to establish baseline standards that ensure legal compliance

but are still broad enough to provide each agency the flexibility to shape management practices to fit their unique requirements.

It should also be noted that e-mail systems, and the number of devices capable of accessing them (cell phone, Blackberry, etc.), will continue to grow in complexity, so related policies and procedures should be reviewed and updated as necessary.

DEFINITIONS

Proprietary and Non-proprietary Formats

Format refers to essential characteristics of an electronic file. E-mail often exists as both an electronic format and a file format. In the case of the file format, these formats are often proprietary, meaning it is controlled and readable only through the software of a single company and thus only on computers that run that software. Since this type of file cannot be exported to any other environment, it is necessary to ensure that e-mails are created in, or can be converted to, non-proprietary formats.

Style Format

RFC 2822 is the international standard applied to the vast majority of e-mails. It defines e-mail as consisting of a header, with routing information, and a body, which contains the message, separated by a blank line. Users may add other features to this format, such as a signature, that will be applied to each e-mail sent. It is essential that the format of e-mails be preserved and that they are viewable as they were created. Some means of saving e-mails, such as plain text, do not preserve the original format, and thus are not ideal for the purposes of records management.

Metadata

E-mail records include not only the text of the message, but all of the accompanying contextual information that the e-mail system tracks, such as who sent it (their full name plus e-mail address), when it was sent, who received it, when it was opened, any distribution lists used, etc. All of these data are called metadata and are just as necessary to the record as is the text. When records are placed in a record-keeping system, the attendant metadata also needs to be stored.

Attachment

Attachment refers to any file which accompanies an e-mail message. Attachments can exist in a large variety of formats (the number of which continues to increase as software is superseded or new software developed) and may be text, graphics, spreadsheets, video, audio files, Web pages, compressed files, or any combination of these mediums. Like e-mails and metadata, the attachments of e-mails must also be retrievable in an unaltered state.

Discovery
Discovery refers to the compulsory disclosure of records believed to be associated with ongoing litigation. Likewise, e-discovery refers to the same process but is focused solely on electronic records, e-mails primary among them. The legal risks associated with discovery and e-discovery make the establishment of a Statewide e-mail management policy all the more crucial. The federal and State rules of procedures now compel civil litigants to preserve and produce electronic evidence on demand.[1]

RECORDS MANAGEMENT AND RECORD-KEEPING SYSTEMS

E-mail records should be placed in some kind of record-keeping system. A record-keeping system can sort records according to purpose and retention schedule, provide security against unauthorized access or destruction, facilitate efficient retrieval, and preserve important information. Once the record is in the system, the original electronic source record that may still exist in the in or out box should be destroyed. Any backup tapes to the e-mail system, containing only duplicates, could then also be destroyed.

E-mail Systems

Until recently, most e-mail management systems relied on the user to organize and purge e-mails via a system of folders or through similar options such as the GroupWise "cabinet." Managing e-mail within electronic folders is technology that is readily available and requires minimal training. Folders within the cabinet are set up according to function and retention category. When an e-mail worth keeping is sent or received, it is moved to the appropriate folder. After the records become inactive, then they are deleted according to their retention schedule or saved in a format that can be transferred to Archives for permanent storage. User-managed folders within an e-mail system are a simple electronic record-keeping system that may conflict with records management policy through employee oversight or negligence or, in some cases, intentional breach of ethics.

Centralized Systems

Software that is purchased, developed, or customized to automate the records management functions offers greater control over when and how records are viewed by an organization (not just the creator), destroyed, or transferred to the State Archives. This type of software centralizes many functions that are then overseen by a professional records manager. Central control of e-mail records management alleviates issues such as duplicates and tends to better organize

[1] Federal Rules of Civil Procedure, Fed. R. Civ. P. 37 "(e) Failure to Provide Electronically Stored Information. Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system."

Utah Rules of Civil Procedure, Utah R. Civ. P. 37 "(g) Failure to preserve evidence. Nothing in this rule limits the inherent power of the court to take any action authorized by Subdivision (b)(2) if a party destroys, conceals, alters, tampers with or fails to preserve a document, tangible item, electronic data or other evidence in violation of a duty. Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system."

extended correspondence among multiple users while also ensuring legal compliance. The oversight of deletion or purging of e-mails from the system is also concentrated among trained records managers as opposed to relying on every employee in each agency to maintain compliance.

There are several centralized e-mail management options available to large operations such as state governments that significantly reduce the risks associated with end-user systems. The first option is a Local Area Network (LAN). LAN storage relies on each user of an e-mail system manually moving individual e-mails out of a mailbox and into the shared file directory structure. This option still leaves the door open to some of the risks associated with end-user management, but it has the advantage of some central oversight, especially in regards to retention and disposition.

A second option is e-mail archiving software, which is capable of organizing incoming and outgoing e-mails and sending them to centralized servers. The benefits of such software lay largely in its automation and in its reduction of the amount of e-mails that need to be stored on individual computers and online servers. The downside to such software is that its focus is solely on e-mails, which necessitates a separate system for other types of electronic records.

A third option is an Electronic Document Managing System for Enterprise Content Management (EDMS/ECM) to act as a central archive for all types of electronic records. Many of these types of systems are capable of both automatically managing e-mail traffic and tracking retention and disposition of e-mails and other types of electronic records.

Agencies may choose whichever record-keeping system fits best working in conjunction with the Department of Technology Services. Recommended functionality requirements that these systems should contain has been prepared by the U.S. Department of Defense, titled the 5015.2 standard.[2]

POLICY COMPONENTS

The goal of an e-mail management system is to manage e-mail from creation or receipt to destruction or permanent preservation. The policy that governs that program must address—but not necessarily be limited to—the following points:

Essential Elements of the E-mail Management System
Require, via policy, administrative rule, or statute, that each State agency uses an approved electronic records management system or develop a policy of their own that is in compliance with the baseline standards of said system. A management system includes the hardware,

[2] Joint Interoperability Test Command, Records Management Application, http://jitc.fhu.disa.mil/recmgt/standards.html. The current version of DoD 5015.02-STD, signed 25 April 2007, defines the basic requirements based on operational, legislative and legal needs that must be met by records management application (RMA) products acquired by the Department of Defense (DoD) and its Components. It defines requirements for RMA's managing classified records and includes requirements to support the Freedom of Information Act (FOIA), Privacy Act, and interoperability. This standard is recommended by the National Archives and Records Administration as well as the Utah State Archives.

software, and storage medium used to manage e-mail, and the policy describes how the system is used and the records it contains. To ensure that all essential e-mails are accessible within the management system, the policy must require that all State business is conducted on computers and devices that are connected to an authorized management system.

Evaluating and Appraising E-mail

Several issues must be considered when determining how e-mails fit within a records management system. The most important of these questions is whether an e-mail is a record. If the e-mail was sent or received as part of a State business transaction, be it an interagency transaction or business with an entity outside of State government, it is considered a record. According to GRAMA, UCA § 63G-2-201(3)(b), a record is:

> *a book, letter, document, paper, map, plan, photograph, film, card, tape, recording, electronic data, or other documentary material, regardless of physical form or characteristics, that is prepared, owned, received, or retained by a governmental entity or political subdivision where all of the information in the original is reproducible by photocopy or other mechanical or electronic means.*

Principally, e-mail that is work-function related, and has administrative, legal, fiscal, or historic value, is a record. Conversely, documents that are considered non-records include: drafts, personal notes or communications, proprietary software, copyrighted material, junk mail, commercial publications, and personal daily calendars. Personal records as defined by UCA § 63G-2-103, created or received through e-mail systems, do not require a formal retention schedule. The recommendation is to destroy upon receiving or sending.

Once an e-mail is determined to be a record, it must be decided whether it is the “record copy” of that correspondence. Since duplicate copies can be discarded at any time, retention schedules are only going to apply to the official record copy of that e-mail. The same kind of consideration should be given to attachments within e-mails. It is important to note that attachments may well have their retention periods, and thus a determination needs to be made regarding whether the attachment exists in other formats (paper, PDF, word-processor file, etc.) and which of the formats is the record copy. Like e-mail, attachments that are duplicates can be discarded when the administrative need of the recipient has ended.

Primarily, within government, the outgoing (sender’s) copy of an e-mail is the record copy, and the copy with the longest retention. This retention holds until a response is made to the initial e-mail, at which point a series of correspondence (thread) is created. In such instances, the last e-mail in the thread—the one containing the entirety of the correspondence between two or more persons—becomes the record copy and thus the copy with the longest retention period. However, e-mail can be broadcast to hundreds of people at once, and each of those duplicates should not be saved. Only those recipients who then respond to the correspondence need save copies. Incoming (the recipient’s) e-mail originating from outside the government is the record copy.

If it is decided that the e-mail is the record copy, then the record series to which it belongs needs to be determined. The record series will indicate the e-mail’s legal retention period and its ultimate disposition (i.e., destroy or permanent preservation and access).

Access and Retrieval
The current method for retrieving and finding e-mail uses the search functionality of the e-mail system. Most employees save e-mails to a file on their assigned computers. These files, as well as live e-mails, can be searched for author or recipient name, time periods, subject as derived from the message title, and a full text search of the e-mail, but not the attachments. To make searching more reliable and efficient, e-mail and related attachments judged to be worth keeping should be ingested into an e-mail records management system that provides faster and enhanced search capabilities.

In order to provide accessibility and promote efficient searching mechanisms, all outgoing e-mails related to State business must have a subject line that clearly reflects the content of the e-mail. Index terms to the metadata may be applied to further promote ease of access.

Disposing of all non-record e-mails greatly reduces the amount of e-mail that requires access and retrieval resources. Some systems provide capabilities for employees to make these categorical decisions rapidly and with high levels of automation. Currently most retention decisions are managed manually at the discretion of the employee and specific agency policies within the context of the current e-mail environment.

E-mail saved on employee machines should not be routinely purged by LAN personnel and should not be automatically discarded upon termination, but preserved until such time that they can be reviewed and appropriate retentions applied to the records. Approved retentions and appropriate disposition for destruction of these types of e-mail should be established to minimize storage requirements for the State.

E-mail system backups should be administered in a manner consistent with the e-mail retention policies of the State and the specialized requirements of the agencies.

E-discovery
Both the federal and Utah Rules of Civil Procedure expressly provide for the discovery in litigation of all discoverable electronically created or stored information, including e-mails, in their electronic format. Electronically stored or created information can be regularly destroyed without penalty under these rules if the destruction was pursuant to a reasonable electronic records management system that is consistently implemented and followed within the agency.

This "safe harbor" is suspended, however, when a "litigation hold" has been, or should have been, put in place. A litigation hold is an internal directive to preserve all relevant information, including electronically created or stored information, which is in the possession, custody, or control of the agency.

The obligation to implement a litigation hold is triggered as soon as the agency knows, or should have known, that litigation regarding the matter at issue was reasonably foreseeable. Once a litigation hold is implemented, all deletion or destruction protocols with regard to electronically created or stored information that may relate to the matter at issue must be immediately

suspended. Those records must thereafter be preserved in their electronic format until any litigation is concluded or the litigation hold is appropriately lifted.

The failure to properly implement a litigation hold where litigation is reasonably foreseeable, or failing to comply with such a hold after it is implemented, can result in significant penalties or sanctions. Such penalties or sanctions can include: payment of the costs of recovering, sorting and producing the lost information from back-up tapes; payment of all or part of the other side's attorneys fees; where the failure to preserve was known and intentional, significant monetary penalties against the agency and/or its officers, managers, and attorneys; an adverse inference jury instruction, advising the jury that it can presume that lost information would have been favorable to the other side; and, in extreme cases, entry of judgment for the other side.

To avoid such sanctions or penalties, the following procedures should be implemented.

- As soon as an employee of an agency becomes aware of pending litigation or of information that suggests the risk of future litigation (i.e. correspondence from former, particularly terminated, employees or correspondence from a patron regarding or resulting from an interaction they perceive as especially egregious), even if the employee believes that such possibility is remote, the employee should report that information to the appropriate manager or supervisor.

- In turn, as soon as a manager or supervisor obtains such information, whether from an employee or independently, that information should immediately be reported to the executive director of the agency, and to agency legal counsel.

- Agency legal counsel, in consultation with the executive director and such others within the agency as may be appropriate, shall make the determination as to whether litigation is, in fact, reasonably foreseeable. If it is, then a litigation hold shall be issued by agency legal counsel to the agency.

As can be seen from the foregoing, upon the issuance of a litigation hold, the electronic records management system must have the ability to identify, segregate, archive, and preserve discoverable electronically created or stored information, including e-mails, in their original electronic format, including all metadata. The electronic records management system must be able to do this without impeding or interfering with the normal operation of the system with regard to records not affected by the litigation hold.

Storage

To enable a capable e-mail archiving and retention practice at the State, provisions should be established for each of the following types of storage required:

- **Category 1**: Centralized e-mail storage for active e-mail (e.g., the last 60 days) with automated retention and destruction rules consistently implemented to minimize excessive storage requirements.
- **Category 2**: Agency or multi-agency storage for active e-mail at the post office level.

- **Category 3**: Centralized transitional storage for all e-mail assigned to specific records groups by agency personnel.
- **Category 4**: Centralized Archive e-mail repository storage for e-mail that has been transferred to the State Archives and assigned to specific record groups and are accessed through a Records Management System.
- **Category 5**: Archival storage for archived e-mail that has been stored on computers used by employees that have terminated their employment with the State for whatever reason.

Storage for Categories 1, 2, and 4 needs to be high speed, high availability, on demand storage environments. Storage for Categories 3 and 5 can be met by less expensive disk and/or tape storage environments. All of these storage environments should be backed up on established schedules using least-cost automated storage procedures. Stored e-mail must also include relevant document attachments.

Retention and Disposition

The practice of deleting e-mail on a regimented schedule of backup tape cycles without regard to content is in contravention of legally established retention schedules. Conversely, the backup tapes may contain information that was disposed of according to an approved retention, thus increasing costs and decreasing efficiency.

Retention schedules are created to account for any administrative, fiscal, legal, or historical value that may be contained in a record so that it may be disposed of appropriately. General retention schedules are designed to cover the needs of common records across all agencies. The following general retention schedules currently are used for various types of correspondence, including e-mail:

Transitory Correspondence: This is business-related correspondence that is routine or transitory in nature and does not offer unique information about agency functions or programs. These records include acknowledgment files and most day-to-day office and housekeeping correspondence. These records may originate on paper, electronic-mail, or other media. This correspondence is filed separately from program and project case files.

Retention:

- Record Copy: Retained by agency until administrative need ends, and then destroy.
- Duplicate Copies: Retain by agency until administrative need ends, and then destroy.[3]

Policy and Program Correspondence: Business-related correspondence which provide unique information about agency functions, policies, procedures, or programs. These records document material discussions and decisions made regarding all agency interests, and may originate on paper, electronic mail, or other media. This correspondence is filed separately from program case files, and project files.

[3] Utah State General Records Retention Schedule, Transitory correspondence (item 1-47).

Retention:

- Record Copy: Permanent; retained by agency until administrative need ends, and then transfer to State Archives with authority to weed.
- Duplicate Copies: Retain by agency until administrative need ends, and then destroy.[4]

Correspondence categories typically are easy to apply, however a more content-based approach to retention schedules—reflecting the widespread subjects and applications reflected in electronic correspondence—for records groups also is needed. Other general retention schedule record series may be more appropriate to specific record groups, such as case files, and agencies may work with the State Archives in establishing unique retention schedules to fit specific needs of their operations

Preservation

Utah law requires that records are accessible for the full extent of their approved retention periods. Preservation of electronic records, including e-mail, even for short-terms can be an issue because of technological changes and media degradation. Open-source solutions are ideal for meeting this requirement.

- One strategy is the use of XML. Essentially, scripts are run against the transmittal copy of the e-mail, with the message, attachments, and metadata captured and wrapped with XML. The XML files then are placed in an electronic recordkeeping system.
- Adopting open source products facilitates migration or conversion of e-mail systems.

Appropriate Use

E-mail within State government is subject to the existing Department of Technology's *Acceptable Use Rule*[5], which establishes guidelines for appropriate use of computing resources and content on State systems. State policy allows some limited personal use of e-mail systems so long as such use is consistent with the *Acceptable Use Rule*. State provided e-mail is considered to be the primary venue for conducting State business, and such business should not be conducted using third party e-mail providers. As a matter of principle, State e-mail users are expected to conform to the following:

- State business conducted via e-mail should use established and approved State e-mail systems.
- Private business activities should never be conducted using State e-mail systems.
- E-mail should respect gender, creed, race, ethnic background, or other identifying characteristics.
- E-mail should be preserved and managed consistent with State records policies and rules.
- E-mail should respect the integrity of computing systems.

[4] Utah State General Records Retention Schedule, Policy and program correspondence (item 1-9).
[5] Title R895. Technology Services, Administration. Rule R895-7. Acceptable Use of Information Technology Resources.

- Individual user accounts and passwords must be safeguarded.

Agency and State e-mail policies should be integrated into existing Web mail and network access policies to strengthen and give visibility to e-mail policies.

THE BACKLOG

Many State agencies have an extensive backlog of e-mails that simply are sitting in servers and in boxes. Due to risks associated with e-discovery and litigation, it is equally important that these records be managed retroactively according to established records retention periods. The scale of backlogged e-mails, and the risks associated with these records, will vary from agency to agency, as will the complexity of bringing them up to newly-established standards.

Once standards for records management are established, those records most at-risk should be prioritized and addressed.

Often backups can be downloaded or e-mails simply relocated to the new, centralized system. In cases of obsolescence or backup failure, data recovery specialists can be contracted to restore information in current formats or mediums.

SUMMARY

E-mail must be managed not as a physical format with one-size-fits-all requirements, but as content that has specific value or non-value to an agency. To manage e-mail, State agencies should work to customize a centrally-managed, open-source, records management system to support their individual needs and obligations. Such a system must address the issues of records evaluation; appraisal and retention; appropriate use; preservation and issues of obsolescence; access and retrieval; and e-discovery.